Claims 1-22. Cancelled.

23. [Currently amended] A secure data-provision method for ~~comprising~~ providing target data from a data provider to a party purporting to be a specific, professionally-accredited, individual engaged by a specific accredited organisation, the target data being provided in encrypted form as part of a data set; ~~that comprises~~ the method comprising:

encrypting a first item ~~encrypted~~, according to an Identifier-Based Encryption, IBE, scheme, in dependence on encryption parameters comprising a first encryption key string that identifies said specific individual, and public data of a first trusted authority competent in respect of professional accreditations; and

encrypting a second item ~~encrypted~~, according to an IBE scheme, in dependence on encryption parameters comprising a second encryption key string that identifies said specific organisation, and public data of a second trusted authority competent in respect of accreditations of organisations; and

forming said data set using at least the encrypted first and second items;

recovery of the target data in clear requiring decryption of both the first and second items.

24. [Original] A method according to claim 23, wherein the first item comprises the target data, and the second item comprises the encrypted first item.

25. [Original] A method according to claim 23, wherein the first item comprises the target data, and the second item comprises a nonce; the first encryption key string comprising, in combination, an identifier of said specific individual and said nonce.

26. [Original] A method according to claim 23, wherein the first item comprises first data, and the second item comprises second data; the data set further comprising said target data encrypted using a symmetric key that can be formed by using both said first and second data.

27. [Original] A method according to claim 23, wherein the data set comprises, in addition to said first and second items, said target data encrypted using a first symmetric key, the second item comprising a second symmetric key, and the first item comprising the first symmetric key encrypted using the second symmetric key.

28. [Currently amended] A secure data-provision method for ~~comprising~~ providing target data from a data provider to a party purporting to be a specific, professionally-accredited, individual engaged by a specific accredited organisation, the target data being provided in encrypted form as part of a data set, the method ~~that comprises~~ comprising:

encrypting a first item ~~encrypted~~ using both a first encryption key string that identifies said specific individual, and public data of a first trusted authority competent in respect of professional accreditations; and

encrypting a second item ~~encrypted~~ using both a second encryption key string that identifies said specific organisation, and public data of a second trusted authority competent in respect of accreditations of organisations; and

forming said data set using at least the encrypted first and second items;

recovery of the target data in clear requiring decryption of both the first and second items.

Claims 29-42. Cancelled.

43. [Original] Apparatus for the secure provision of target data to a party purporting to be a specific, professionally-accredited, individual engaged by a specific accredited organisation, the apparatus comprising an encryption subsystem for generating a data set including the target data in encrypted form, the encryption subsystem comprising:

first encryption means for encrypting a first item, according to an Identifier-Based Encryption, IBE, scheme, based on encryption parameters comprising a first encryption key string that identifies said specific individual, and public data of a first trusted authority competent in respect of professional accreditations;

second encryption means for encrypting a second item, according to an IBE scheme, based on encryption parameters comprising a second encryption key string that identifies said specific organisation, and public data of a second trusted authority competent in respect of accreditations of organisations; and

means for forming the data set using at least the encrypted first and second items; the recovery of the target data in clear requiring decryption of both the first and second items.

44. [Original] Apparatus according to claim 43, wherein the first item comprises the target data, and the second item comprises the encrypted first item.

45. [Original] Apparatus according to claim 43, wherein the first item comprises the target data, and the second item comprises a nonce; the first encryption key string comprising, in combination, an identifier of said specific individual and said nonce.

46. [Original] Apparatus according to claim 43, wherein the first item comprises first data, and the second item comprises second data; the data set further comprising said target data encrypted using a symmetric key that can be formed by using both said first and second data.

47. [Original] Apparatus according to claim 43, wherein the data set comprises, in addition to said first and second items, said target data encrypted using a first symmetric key, the second item comprising a second symmetric key, and the first item comprising the first symmetric key encrypted using the second symmetric key.

48. [Original] A computing entity for recovering target data provided in encrypted form as part of an data set that comprises first and second encrypted items both of which

must be decrypted to recover the target data, the first item being encrypted in dependence on encryption parameters comprising a first encryption key string that identifies a specific individual and first public data, and the second item being encrypted in dependence on a second encryption key string that identifies a specific organisation and second public data; the entity comprising:

first means for requesting either a first decryption key corresponding to the first encryption key string, or the first item in decrypted form, from a first trusted authority which is competent in respect of the accreditation of professionals and holds first private data related to the first public data, the first means being arranged to provide the first encryption key string to the first trusted authority when making its request and being further arranged to authenticate the entity with the first trusted authority and to receive the first decryption key, or the first item, securely from the first trusted authority;

second means for requesting either a second decryption key corresponding to the second encryption key string, or the second item in decrypted form, from an organisation accredited by a second trusted authority which holds second private data related to the second public data, the second means being arranged to provide the second encryption key string to the organisation when making its request and being further arranged to authenticate the entity with the organisation and receive the second decryption key, or the second item, from the organisation;

third means for using the first decryption key, or the first item, provided by the first trusted authority and the

second decryption key, or the second item, provided by the organisation, to recover the target data.

49. [Original] A computing entity according to claim 48, wherein the second means is arranged to receive the second decryption key, or the second item, securely from the organisation.

50. [Original] A computing entity according to claim 48, wherein the first item comprises the target data, and the second item comprises the encrypted first item; the third means being arranged to: recover the second item, if not provided to the second means in decrypted form by the organisation, by using the second decryption key obtained from the organisation, and subject the second item to decryption, using the first decryption key obtained from the first trusted authority, to recover the target data.

51. [Original] A computing entity according to claim 48, wherein the first item comprises the target data, the second item comprises a nonce, and the first encryption key string comprises, in combination, an identifier of said specific individual and said nonce; the third means being arranged to: recover the second item, if not provided to the second means in decrypted form by the organisation, by using the second decryption key obtained from the organisation, combine the nonce that formed the second item with the identifier of said specific individual in order to form the first encryption key string to be provided by the first means to the first trusted authority, and use the first decryption key obtained from the first trusted

authority to decrypt the first item and thereby recover the target data.

52. [Original] A computing entity according to claim 48, wherein the first item comprises first data and the second item comprises second data, the data set further comprising said target data encrypted using a symmetric key that can be formed by using both said first and second data; the third means being arranged to recover the first data, if not provided to the first means by the first trusted authority, by using the first decryption key obtained from the first trusted authority, recover the second data, if not provided to the second means in decrypted form by the organisation, by using the second decryption key obtained from the organisation, use the first data and the second data to form said symmetric key, and use the symmetric key to decrypt the target data.

53. [Original] A computing entity according to claim 48, wherein the data set comprises, in addition to said first and second items, said target data encrypted using a first symmetric key, the second item comprising a second symmetric key, and the first item comprising the first symmetric key encrypted using the second symmetric key; the third means being arranged to: recover the first item, if not provided to the first means by the first trusted authority, by using the first decryption key obtained from the first trusted authority, recover the second item, if not provided to the second means in decrypted form by the organisation, by using the second decryption key obtained from the organisation, use the second symmetric key that

formed the second item to decrypt the encrypted first symmetric key that formed the first item, and use the first symmetric key to decrypt the encrypted target data.

54. [Original] A computing entity for recovering target data provided in encrypted form as part of an data set that comprises first and second encrypted items both of which must be decrypted to recover the target data; the first item being encrypted in dependence on a first encryption key string that identifies a specific individual, and first public data; and the second item being encrypted in dependence on a second encryption key that identifies a specific organisation and said specific individual, and second public data; the entity comprising:

first means for requesting either a first decryption key corresponding to the first encryption key, or the first item in decrypted form, from a first trusted authority which is competent in respect of the accreditation of professionals and holds first private data related to the first public data, the first means being arranged to provide the first encryption key string, or the first item, to the first trusted authority when making its request;

second means for requesting either a second decryption key corresponding to the second encryption key string, or the second item in decrypted form, from an organisation accredited by a second trusted authority which holds second private data related to the second public data, the second means being arranged to provide the second encryption key string to the organisation when making its request; and

third means for using the first decryption key, or the first item, provided by the first trusted authority and the

second decryption key, or the second item, provided by the organisation, to recover the target data;

at least one of the first means and the second means being arranged to authenticate the entity to the first trusted authority or said organisation as the case may be and to receive input therefrom in a secure manner.

55. [Original] A computing entity according to claim 54, wherein the first item comprises the target data, and the second item comprises the encrypted first item; the third means being arranged to: recover the second item, if not provided to the second means in decrypted form by the organisation, by using the second decryption key obtained from the organisation, and subject the second item to decryption, using the first decryption key obtained from the first trusted authority, to recover the target data.

56. [Original] A computing entity according to claim 54, wherein the first item comprises the target data, the second item comprises a nonce, and the first encryption key string comprises, in combination, an identifier of said specific individual and said nonce; the third means being arranged to: recover the second item, if not provided to the second means in decrypted form by the organisation, by using the second decryption key obtained from the organisation, combine the nonce that formed the second item with the identifier of said specific individual in order to form the first encryption key string to be provided by the first means to the first trusted authority, and use the first decryption key obtained from the first trusted

authority to decrypt the first item and thereby recover the target data.

57. [Original] A computing entity according to claim 54, wherein the first item comprises first data and the second item comprises second data, the data set further comprising said target data encrypted using a symmetric key that can be formed by using both said first and second data; the third means being arranged to recover the first data, if not provided to the first means by the first trusted authority, by using the first decryption key obtained from the first trusted authority, recover the second data, if not provided to the second means in decrypted form by the organisation, by using the second decryption key obtained from the organisation, use the first data and the second data to form said symmetric key, and use the symmetric key to decrypt the target data.

58. [Original] A computing entity according to claim 54, wherein the data set comprises, in addition to said first and second items, said target data encrypted using a first symmetric key, the second item comprising a second symmetric key, and the first item comprising the first symmetric key encrypted using the second symmetric key; the third means being arranged to: recover the first item, if not provided to the first means by the first trusted authority, by using the first decryption key obtained from the first trusted authority, recover the second item, if not provided to the second means in decrypted form by the organisation, by using the second decryption key obtained from the organisation, use the second symmetric key that

formed the second item to decrypt the encrypted first symmetric key that formed the first item, and use the first symmetric key to decrypt the encrypted target data.